THE ARTIFACT IDENTITY PROBLEM

Why the Internet Needs Portable File Identity

Abstract v1.4

In the long evolution of Internet security, Portable File Identity may represent the moment when trust moved from the systems that store information to the artifacts that carry it.

VeraSec Technologies

Brian Hajost
bhajost@verasec.net

About VeraSec Technologies

VeraSec Technologies is a pioneer in digital artifact integrity, focused on moving the security context from the infrastructure directly to the file itself. While traditional security models rely on centralized systems to establish and maintain trust, VeraSec's patent-pending technologies empower files to carry their own verifiable identity - preparing them for an actual Zero Trust world.

Operating at the forefront of Portable File Identity (PFI), VeraSec invented the Validation Integrity Key (VIK) process. This innovation patches a fundamental vulnerability in traditional PKI that has persisted for decades. By cryptographically binding a file's content and metadata into a compact, human-readable identifier embedded directly within the artifact, VeraSec helps organizations establish durable, portable trust in every digital asset, signed or un-signed - wherever it travels.

About The Author

Brian Hajost is a cybersecurity entrepreneur and technologist with more than 30 years of experience in information security, compliance automation, and trusted computing systems.

As the founder of SteelCloud, he pioneered the automation of DISA STIG and CIS benchmark compliance for the DoD, federal agencies, and enterprise customers. Brian holds 15 patents in information technology and mobile security. In 2022 he was named one of the "Top 10 Most Influential People in Cyber Security" by CIO Views.

His current work focuses on solving what he describes as the Artifact Identity Problem - the absence of durable identity for files as they move across distributed systems and untrusted networks.

The Artifact Identity Problem

Why the Internet Needs Portable File Identity

Executive Summary

Modern computing depends on digital artifacts. Documents, software packages, datasets, and logs move continuously across systems and organizational boundaries. Yet, despite their central role, most artifacts lack a durable identity. When a file leaves its native environment, the infrastructure that established its authenticity - metadata, access controls, and repository context, stays behind.

The *Artifact Identity Problem* describes this architectural gap. This paper argues for a new security layer: Portable File Identity (PFI). By allowing artifacts to carry cryptographically derived, human-readable identity markers, we can establish durable trust that travels with the file, anywhere it goes.

---

1. The Internet's Architectural Blind Spot

The original Internet was designed for communication, not content persistence. Protocols like TCP/IP solved the problem of moving packets; later, TLS and PKI secured the "handshake" between hosts. More recently, Zero Trust architectures have refined how we verify users and devices.

However, these mechanisms secure the interaction, not the object. Files - the primary vessels of global information, remain passive containers. They can be renamed, compressed, or redistributed without retaining any inherent proof of origin. This was acceptable in a siloed world, but in a hyper-distributed ecosystem, the absence of artifact identity is a fundamental flaw in the Internet's trust architecture. As artifacts travel farther from their original context, the absence of durable identity becomes an increasingly significant weakness.

---

2. Infrastructure Doesn't Travel; Files Do

In modern workflows, a file is a nomad. A document born in a secure enterprise repository is emailed to a partner, downloaded to a personal device, archived in a public cloud, and shared via Slack.

The security controls (IAM, audit logs, EDR) exist only within the "walls" of the originating system. Once the file is exported, it becomes a "stranger." The farther a file moves from

its point of origin, and the more time elapses, the more its identity erodes into uncertainty. The artifact persists, and the controlled infrastructure persists - but they are permanently divorced from one another.

---

3. The Cost of Anonymous Artifacts

When artifacts are anonymous, authenticity is an expensive guessing game. This gap facilitates:

- Shadow Versions: Two files with the same name but different contents.
- Impersonation Attacks: Malicious binaries disguised as legitimate software.
- Context Loss: The inability to prove a file is the "Golden Version" once it's in a third-party environment.

Currently, we try to "reconstruct" trust using external hash databases or digital signatures. While useful, these are brittle. They require the recipient to have the same specialized tools, certificate chains, or database access as the sender. If the validation infrastructure isn't present, the trust evaporates. And these security measures are unavailable or inappropriate for many types of artifacts.

The result is a digital ecosystem in which the authenticity of many artifacts is uncertain. Files continue to circulate widely, but the ability to verify their identity often depends on external context that may be incomplete, unavailable, or difficult to reconstruct.

This ambiguity creates a persistent vulnerability in modern computing systems.

---

4. The Limits of Existing Integrity Mechanisms

A range of established technologies attempt to address artifact integrity, including PKI-based digital signatures, cryptographic hashing, and enterprise control frameworks. While each provides meaningful assurances, their effectiveness is largely constrained to the environments in which they are created and enforced.

As files move out from their controlled environments, these mechanisms often degrade. Signatures may not be consistently validated, hashes become detached from the artifact, and infrastructure-dependent controls lose visibility and enforcement.

Portable File Identity (PFI) addresses this gap. By embedding a persistent, verifiable identity directly with the file, PFI not only extends trust beyond infrastructure boundaries, but also reinforces the integrity of existing mechanisms - enabling continuous validation of signatures, detection of tampering, and preservation of artifact integrity regardless of where the file travels.

Mechanism	Strength	Weakness
Hashing	Mathematical certainty of equality	Requires a reference "known good" hash from an external source
Digital Signatures	Provides the identity of the signer	Heavy dependency on PK/CA infrastructure, easily removed, only covers a portion of the file
File Repository Security	Strong internal version control	Trust ends the moment the "export/download" button is pushed

5. The Vision: Portable File Identity (PFI)

Several technologies attempt to address aspects of artifact integrity, but each has limitations once files move beyond the systems and infrastructure that created them. Portable File Identity (PFI) shifts the focus from **infrastructure-based trust** to **object-based trust**.

PFI is a cryptographically derived identifier generated at the moment of the file's creation or "sealing" within a trusted environment. It transforms the file from a passive data container into a **self-identifying artifact**.

Key Characteristics of PFI:

1. **Deterministic:** The identity is derived from the file itself.
2. **Infrastructure-Independent:** Any system can re-verify the identity without calling back to the originating server.
3. **Durable:** The identity travels *with* the file, embedded in the name or metadata.
4. **Human-Readable:** Unlike a 64-character hex string, PFI can be represented as a compact, recognizable marker that allows humans to spot discrepancies at a glance.

6. The Human-Readable Advantage

A unique pillar of PFI is bridging the gap between machine verification and human intuition. By making the identity marker visible (e.g., in the filename or a tag), users gain situational awareness.

Machines perform the precise cryptographic check, but humans can visually confirm they are looking at the correct version of a document or a software patch. This visibility provides a practical safety net. By combining cryptographic integrity with human-readable representation, Portable File Identity bridges a longstanding gap between security mechanisms and human workflows - enabling artifacts to carry trust information that can be recognized by systems and people alike.

7. Cybersecurity Implications: Sealing the Supply Chain

If PFI is implemented at scale, the defensive landscape changes:

- **Instant Tamper Detection:** Any change to the file - intentional or accidental, breaks the identity validation link.
- **Mitigating Substitution:** Attackers cannot replace a legitimate file with a malicious one without the identity marker changing.
- **Automated Integrity Audits:** Security tools can scan petabytes of data, validating PFI markers instantly without needing to query a central "source of truth.".
- **High-Volume Log protection:** Machine-generated artifacts (telemetry, logs) can be "sealed" at the edge, at enterprise speeds, ensuring their integrity for future forensic audits.

Conclusion

Every security model in widespread use relies on non-repudiation. It is a core principle of secure design. In each technology, a mechanism of trust is carried along: a checksum is passed with the packet, a nonce is passed with the wireless handshake, and an SSL certificate is loaded into a website. Yet, for decades, the file has carried nothing: no protected identity, no provenance, and no memory of who created it or what policies governed it. The Artifact Identity Problem is not just a technical oversight; it is a fundamental vulnerability in how we secure global information. The artifact is the only component of the modern security stack that cannot reliably answer the question, ***"Who are you?"***

Portable File Identity provides the definitive answer. PFI transforms files from passive data containers into self-validating objects, bridging the most glaring gap in modern cybersecurity. Files are the primary currency of the Internet, yet they have remained their most anonymous citizens. In the long evolution of Internet security, Portable File Identity represents the crucial moment when trust finally shifts from the infrastructure that stores information to the artifacts that carry it.